UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/779,535	02/13/2004	Eric John Anderholm	SGTL-0001-P60	5595

43520 7590 04/07/2008

STRATEGIC PATENTS P.C..
C/O PORTFOLIOIP
P.O. BOX 52050
MINNEAPOLIS, MN 55402

EXAMINER	
LASHLEY, LAUREL L	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
04/07/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/779,535	ANDERHOLM ET AL.	
	Examiner	Art Unit	
	LAUREL LASHLEY	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-53* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-53* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 February 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1 – 53 are pending and have been examined.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 01/07/200, 02/14/2005, and 12/07/2005 was filed before the mailing date of any first Office Action on merits. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Drawings

3. The drawings were received on 02/14/05. These drawings are acceptable.

Specification

4. The amendments to the specification were received on 02/14/05. These amendments are acceptable and have been entered.

Claim Objections

5. Claims 25-35 are objected to because of the following informality:

i. Claim 25 recites "coman agent" where it is believed it should read --command agent-- or --common agent--. Claims not specifically identified are objected to by virtue of dependency. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1-2, 4-10,12-18,20-26,30-36,40-46, and 48-53 rejected under 35 U.S.C. 102(b) as being clearly anticipated by Houston et al. in US PGPub No. 2002/0019945 (hereinafter Houston).

7. For claim 1, and similar claims 10, 18, 25, 36, 46 and 53, Houston discloses:

A method of managing security in an enterprise, comprising: (see Abstract, lines 1-2)

detecting at periodic intervals events that correspond to user interactions with computers connected to a network of the enterprise; (see Abstract, lines 2-5: event managing software module monitors network activity)

storing such events in a data facility; organizing the events by user, by computer and by event type (see Abstract, lines 5-6,11: collect and store events); and

presenting a summary of the events in a report, wherein a viewer of the report may select the organization of the report by user, by computer and by event type (see Abstract, lines 8-10: format and create; Abstract, lines 11-12: results). (see also [0007] –[0008])]

For claim 2 and similar claim 26, Houston discloses:

A method of claim 1, wherein the report is in a graphical format. (see Figure 15; [0009], lines 10-13: graphical format)

For claim 4 and similar claims 12, 20, 30, 40, and 48, Houston discloses:

A method of claim 1, wherein the events are selected from the group consisting of keyboard event, a mouse event, an intellipoint event, a trackball event, a cursor event, a screen event, sensor event, a touchpad event, a tablet event, a touchscreen event, a joystick event, a pen event, a voice recognition event, and biometric event. (see Figure 1, [0041]: security device monitoring various points on network; Figure 20, 21: additional events details; [0044]: monitor events data using selected scopes)

For claim 5 and similar claims 13, 21, 31, 41 and 49, Houston discloses:

A method of claim 1, wherein the user is selected from the group consisting of an employee, a consultant, a teacher, a student, a government official, a patient, a volunteer, an attendant, a team member, a system administrator, a contractor, a vendor, a clerk, a cashier, a teller, a comptroller, an accountant, an attorney, a financial officer, a principal, an administrator, a human resources employee, a broker, a gaming employee, a guard, a banker, a government official, a trustee, a guardian, a steward, an authorized user and a non-authorized user. (see [0003]: LANS used by companies, users of events manager: schools, organizations other enterprises; Figure1: client 115)

For claim 6 and similar claims 14, 32, and 42, Houston discloses:

A method of claim 1, wherein the report relates to compliance with a policy of the enterprise. (see Abstract; [0052]: inherent in network security management)

For claim 7 and similar claim 33, Houston discloses:

A method of claim 1, wherein the report relates to security of the enterprise. (see Abstract: lines 1-2)

For claim 8 and similar claim 34, Houston discloses:

A method of claim 1, wherein the report relates to performance of an objective of the enterprise. (see Abstract; [0052]: inherent in network security management)

For claim 9 and similar claim 17, 24, 35, 45, and 52, Houston discloses:

A method of claim 1, wherein the report relates to content viewed by the user, the content selected from the group consisting of chat room content, content relating to securities, insider trading information, content relating to gaming, pornographic content, illegal content, vulgar content, prurient content, gambling content, entertainment content, video game content, trade secret content, proprietary content, engineering content, drug-related content,

health-related content, a medical record, a patient record, a financial record, account information, educational information, indication of harassment, indication of a crime, indication of policy or regulatory non- compliance, identification of a competitive entity, identification of an adverse entity, identification of a specific individual, transcript information, access to an employment-oriented website, content designated prohibited by policy, and trading information. (see Figure 20: exemplary grouping of types of security events)

For claim 15 and similar claim 43, Houston discloses

A method of claim 10, further comprising sending an alert if a user is suspected of committing a security violation based on the user interactions with the computer. (see Figure 2, items 255,260; [0007], lines 16-17: respond to security event; [0042]: message module)

For claim 16 and similar claim 44, Houston discloses

A method of claim 10, further comprising increasing the rate of capture of user interactions if a user is suspected of committing a security violation. (see [0007],[0042], lines 30-35: significant event…incident response)

For claim 22 and similar claim 50, Houston discloses

A method of claim 18, wherein the event relates to an employee's usage of the Internet. (see [0009]: exemplary…creating and applying filtering criteria…analyzing security event…)

For claim 23 and similar claim 51, Houston discloses

A method of claim 22, further comprising providing an alert if an employee's usage of the Internet exceeds a predetermined amount during a predetermined period of time. . (see [0007], [0009], [0042], lines 30-35: significant event…incident response)

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 3, 11, 19, 27-29, 37-39 and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Houston further in view of Nguyen et al in US PGPub No. 20040064731 (hereinafter Nguyen).

For claim 3 and similar claims 11, 19, 27, 37 and 47, Houston discloses the method of independent claims but does not expressly teach limiting access to the report based on a predetermined level of authority of the party seeking access.

Nguyen however does disclose limiting access to the report based on a predetermined level of authority of the party seeking access. (see [0036]-[0037]: role-based management component)

For claim 3 and similar claims 11, 19, 27, 37 and 47 Houston and Nguyen are analogous art because they are from the same field of endeavor (monitoring and managing security events within a computer network). It would be obvious to one of ordinary skill in the art at the time of the invention to modify the reports of the security event managing method of Houston such that it would restrict access to the reports based on authorized users as in Nguyen. The motivation for doing so would to maintain security (i.e. intentional or unintentional modification) and privacy within the security events management system.

Official Notice

9. For claim 28 and similar claim 38, and claim 29 and similar claim 39, Houston and Nguyen discloses the systems of the independent claims but does not expressly disclose the security facility comprising an encryption facility or a password.

However, the Examiner takes Official Notice of the security facility being security ready (e.g. encryption ready or password-protected) since restricting a user's actions to their designated roles by implementing security functions such as encryption and password protection is conventional and well known in the art as availability and integrity features.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Young et al. in US PGPub No. 2004/0168086 discloses interactive security risk management. Proctor in US Patent No. 6530024 discloses an adaptive feedback security system and method.

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to LAUREL LASHLEY whose telephone number is (571)272-0693. The examiner can normally be reached on Monday - Thursday, alt Fridays btw 7:30 am & 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, Jr. can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Laurel Lashley
Examiner
Art Unit 2132

/L. L./
29 March 2008

/Benjamin E Lanier/
Primary Examiner, Art Unit 2132